

Seguridad de la Información Oficina de Transito Departamental del Magdalena: Ausencia de Políticas, Capacitación y Segmentación de Red.

Trabajo final presentado por:	Ing. Ramiro Vega Balaguera Ing. Erica Ortiz Rivas
Programa:	Especialización de Ciberseguridad
Docente:	Fabricio Echeverría Briones
Fecha:	04-08-2026

Índice de contenidos

Resumen	4
Abstract	5
1. Introducción	7
1.1. Objetivo General.....	7
1.2. Objetivos Específicos	8
1.3. Metodología	8
1.3.1. Identificación y Análisis del Problema.....	9
1.3.2. Planificación de la Solución	10
2. Identificación y descripción un problema al interior de la organización	10
2.1. Descripción de la empresa a intervenir.....	12
2.1.1. Misión	12
2.1.2. Visión	12
2.1.3. Mapa de procesos	13
2.1.4. Descripción del proceso a intervenir.....	15
2.1.5. Descripción del problema que presenta el proceso.....	16
3. Establecimiento de planes de acción para la solución del problema	17
3.1. Establecimiento de objetivos	18
3.2. Descripción de la solución	18
3.3. Secuencia de actividades para ejecución de la solución	19
3.4. Descripción de recursos necesarios para la ejecución de la solución.....	20
4. Definición del alcance de la solución, partes interesadas, cronograma y presupuestos. 22	
4.1. Alcance final de la solución	23
4.2. Identificación de responsables de las actividades para ejecución.....	24
4.3. Cronograma de ejecución.....	24

4.4.	Presupuesto.....	26
5.	Referencias bibliográficas	28

RESUMEN

El presente proyecto de aplicación, desarrollado bajo la metodología de investigación-acción, tiene como propósito el diseño de una propuesta de fortalecimiento de la seguridad de la información para la Oficina de Tránsito Departamental del Magdalena, dependencia de la Gobernación del Magdalena encargada de la gestión de trámites relacionados con el tránsito y transporte en el departamento. A partir del diagnóstico del proceso de Gestión de Tecnologías de la Información, se identificaron brechas relacionadas con la ausencia de lineamientos formales para la gestión de credenciales y contraseñas, actualización de aplicaciones y software, copias de seguridad (backup), uso seguro de dispositivos móviles y capacitación del personal de la oficina. También se evidenció la ausencia de una segmentación lógica de la red mediante VLAN que permita separar los equipos de la Oficina de los dispositivos utilizados por usuarios invitados de otras dependencias de la Gobernación. El análisis de estas condiciones se realizó tomando como referencia los controles aplicables del Anexo A de la norma ISO/IEC 27001:2022, los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y las disposiciones legales aplicables en materia de seguridad de la información y protección de datos.

Con base en las brechas identificadas, se diseñó una propuesta que integra tres componentes principales: una propuesta de política de seguridad de la información que contempla lineamientos para la gestión de credenciales y contraseñas, actualización de software y aplicaciones, copias de seguridad y uso seguro de dispositivos móviles; una propuesta de segmentación lógica de la red mediante VLAN y reglas de acceso; y un programa de capacitación y concientización en seguridad de la información para el personal de la Oficina.

El alcance del proyecto comprende exclusivamente el diagnóstico, diseño, documentación y validación de estas propuestas, por lo que no contempla la adquisición de recursos, configuración de equipos, implementación de VLAN, puesta en funcionamiento de políticas, ejecución de copias de seguridad ni realización de jornadas de capacitación. Como resultado, se obtiene una propuesta estructurada que establece lineamientos, procedimientos y recomendaciones para el fortalecimiento de los controles de seguridad de la información y que podrá servir como base para una eventual implementación futura por parte de la entidad y las áreas responsables de las tecnologías de la información.

Palabras clave: seguridad de la información, gestión de riesgos, ISO/IEC 27001, segmentación de red, política de seguridad, capacitación, credenciales.

ABSTRACT

This applied research project, developed using an action research methodology, aims to design a proposal to strengthen information security for the Magdalena Departmental Transit Office, a branch of the Magdalena Governor's Office responsible for managing transit and transportation-related procedures in the department. Based on a diagnostic assessment of the Information Technology Management process, gaps were identified related to the lack of formal guidelines for managing credentials and passwords, updating applications and software, performing backups, ensuring the secure use of mobile devices, and training office staff. The project also revealed the absence of logical network segmentation using VLANs, which would separate the office's equipment from devices used by guest users from other departments within the Governor's Office. The analysis of these conditions was conducted using as a reference the applicable controls of Annex A of the ISO/IEC 27001:2022 standard, the guidelines of the Information Security and Privacy Model (MSPI), and the applicable legal provisions regarding information security and data protection.

Based on the identified gaps, a proposal was designed that integrates three main components: a proposed information security policy that includes guidelines for credential and password management, software and application updates, backups, and secure use of mobile devices; a proposal for logical network segmentation using VLANs and access rules; and an information security training and awareness program for Office personnel.

The scope of the project exclusively includes the diagnosis, design, documentation, and validation of these proposals; therefore, it does not include the acquisition of resources, equipment configuration, VLAN implementation, policy activation, backup execution, or training sessions. As a result, a structured proposal is obtained that establishes guidelines, procedures and recommendations for strengthening information security controls and that can serve as a basis for eventual future implementation by the entity and the areas responsible for information technologies.

Keywords: information security, risk management, ISO/IEC 27001, network segmentation, security policy, training, credentials.

1. INTRODUCCIÓN

Este proyecto de aplicación en investigación-acción se centró en la identificación y resolución de describa la Oficina de Transito Departamental del Magdalena, permitiendo integrar teoría y práctica en un entorno real. Mediante un enfoque de investigación-acción, se desarrollaron habilidades de diagnóstico, análisis y planificación orientadas a mejorar la eficiencia y efectividad de un proceso crítico en la organización. La estructura del proyecto incluyó una revisión exhaustiva del contexto organizacional y la implementación de una solución factible que responde a las necesidades de la organización y optimiza su desempeño.

1.1. OBJETIVO GENERAL

El objetivo principal del proyecto es diseñar una solución operativa al problema de seguridad de la información que se presenta en la Oficina de Transito de la Gobernación del Magdalena, mediante la identificación y análisis de las brechas existentes entre las medidas de seguridad actualmente implementadas y los controles necesarios para proteger los servicios y activos tecnológicos propios de la entidad.

Para ello, se evaluarán las condiciones actuales relacionadas con:

- Políticas de credenciales y contraseñas.
- Políticas de actualización de aplicaciones y software.
- Segmentación de redes.
- Políticas de uso de dispositivos móviles.
- Políticas de copias de seguridad.
- Capacitación del personal en temas de seguridad de información.

La identificación y evaluación de las brechas y vulnerabilidades encontradas servirán como base para el **diseño de una solución de seguridad de la información**, orientada a fortalecer los controles internos, reducir la superficie de ataque y establecer medidas de protección adecuadas para los activos tecnológicos que se encuentran bajo la administración de la entidad.

1.2. OBJETIVOS ESPECÍFICOS

Los objetivos específicos se formulan bajo criterios SMART (específicos, medibles, alcanzables, relevantes y con tiempo definido), de manera que cada uno cuente con un indicador de verificación al cierre del proyecto:

1. Diagnosticar las causas raíz y los impactos asociados a las vulnerabilidades identificadas en el proceso de Gestión de Tecnologías de la Información de la Oficina de Tránsito Departamental del Magdalena, mediante un análisis de brecha (GAP) frente a los controles aplicables del Anexo A de la norma ISO/IEC 27001:2022 y una valoración de riesgos de seguridad de la información, con el propósito de determinar las principales brechas, riesgos y necesidades de tratamiento.
2. Diseñar políticas y procedimientos de seguridad de la información para la Oficina de Tránsito Departamental del Magdalena, orientados a la gestión de credenciales y contraseñas, actualización de software y aplicaciones, copias de seguridad y uso seguro de dispositivos móviles, con el propósito de establecer lineamientos que permitan reducir la exposición a vulnerabilidades y fortalecer la protección de los activos de información bajo administración de la Oficina.
3. Diseñar una propuesta integral de fortalecimiento de los controles de seguridad de la información de la Oficina de Tránsito Departamental del Magdalena, que contemple la segmentación lógica de la red mediante VLAN y reglas de acceso, así como un programa de capacitación y concientización dirigido al personal sobre prácticas seguras, manejo de información, phishing, dispositivos móviles y reporte de incidentes, con el propósito de reducir los riesgos asociados a la infraestructura de red y al factor humano.

1.3. METODOLOGÍA

El proyecto se desarrolló mediante la metodología de investigación-acción, la cual facilitó una colaboración continua entre los dos integrantes del equipo de estudiantes y el docente asesor a lo largo del proceso, permitiendo validar y ajustar los hallazgos obtenidos sobre la Oficina de Tránsito de la Gobernación del Magdalena. Esta metodología proporcionó un enfoque sistemático para identificar el problema de seguridad de la información de la entidad, formular hipótesis sobre sus causas y proponer soluciones fundamentadas en un contexto real, ajustando las estrategias conforme se profundizaba en el diagnóstico. La investigación-acción ofreció así un marco flexible y participativo para ejecutar el proyecto de manera estructurada, generando una intervención bien fundamentada y con alto potencial de impacto para la entidad.

El desarrollo del proyecto se estructuró en tres etapas secuenciales, cada una de las cuales aborda un aspecto específico de la intervención en la Oficina de Tránsito Departamental del Magdalena. En la primera etapa —desarrollada en el presente documento— se identificó y analizó el problema organizacional, incluyendo una descripción detallada de la entidad, su misión, visión y el proceso de gestión de tecnologías de la información afectado. La segunda etapa se centrará en la planificación de la solución, estableciendo objetivos y actividades concretas para el fortalecimiento de las políticas de seguridad, gestión de credenciales, copias de seguridad, uso de dispositivos móviles, capacitación del personal y la segmentación de la red. En la tercera etapa se definirán aspectos operativos como el cronograma, el presupuesto y la asignación de responsables.

1.3.1. Identificación y Análisis del Problema

En la primera etapa, se realizó un análisis exhaustivo de la organización y del contexto en el cual se desarrolla el proceso afectado. Se documentó el problema identificando sus causas raíz, efectos y puntos críticos que afectaban el desempeño del proceso. Este diagnóstico inicial fue esencial para estructurar la solución y asegurar que la intervención respondiera de manera precisa a las necesidades de la organización.

El diagnóstico se desarrolló mediante la revisión de la documentación y lineamientos disponibles relacionados con la gestión de tecnologías de la información de la Oficina de Tránsito Departamental del Magdalena, teniendo en cuenta que la dependencia no cuenta con un documento formal propio que establezca una política de seguridad de la información. Asimismo, se realizaron entrevistas no estructuradas con el personal encargado de la gestión de tecnologías de la información y se efectuó observación directa de las prácticas relacionadas con la gestión de credenciales y contraseñas, actualización de aplicaciones y software, segmentación de la red, uso de dispositivos móviles, gestión de la información y demás controles de seguridad identificados durante el estudio. Los hallazgos obtenidos fueron contrastados con los controles aplicables del Anexo A de la norma ISO/IEC 27001:2022 y los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC, utilizando como marco jurídico complementario las disposiciones aplicables de la Ley 1581 de 2012 y la Ley 1273 de 2009, con el propósito de identificar las brechas existentes, determinar

los riesgos asociados y establecer las bases para el diseño de la solución de seguridad de la información.

1.3.2. Planificación de la Solución

En la segunda etapa, se desarrolló un plan de acción detallado que incluyó la definición de objetivos específicos y una secuencia de actividades que permitiría mitigar o resolver el problema identificado. Esta fase incluyó el diseño de una estrategia de ejecución organizada y estructurada que facilitara el logro de los objetivos propuestos y maximizara la eficiencia del proceso intervenido. La planificación detallada de actividades y recursos fue clave para asegurar una implementación precisa y efectiva.

1.3.2.1. Definición de Alcance y Recursos

La tercera etapa se enfocó en delimitar el alcance de la intervención y los recursos necesarios. Se establecieron responsables para cada actividad, y se elaboró un cronograma de ejecución para controlar el avance de la implementación. Asimismo, se desarrolló un presupuesto que detalló los costos asociados a cada fase, permitiendo optimizar la asignación de recursos. Esta fase aseguró que todas las variables críticas estuvieran alineadas para una ejecución sin interrupciones.

2. IDENTIFICACIÓN Y DESCRIPCIÓN UN PROBLEMA AL INTERIOR DE LA ORGANIZACIÓN

La Gobernación del Magdalena es la entidad territorial encargada de la administración pública del departamento, prestando servicios a la ciudadanía y coordinando la gestión de sus dependencias internas mediante diferentes procesos y sistemas de información. Entre estas dependencias se encuentra la Oficina de Tránsito Departamental del Magdalena, encargada de gestionar diferentes servicios relacionados con el tránsito y transporte, entre los que se encuentran:

- Siniestralidad: digitalizar y gestionar la información relacionada con los accidentes de tránsito ocurridos en las vías del departamento del Magdalena.
- Prevención y sensibilización: desarrollar acciones orientadas a disminuir la tasa de siniestralidad, mortalidad y morbilidad asociada a los accidentes de tránsito en el departamento.

- Comparendos: gestionar y digitalizar la información relacionada con los comparendos de tránsito.
- Audiencias: garantizar el debido proceso y el derecho a la defensa de los presuntos infractores que, con ocasión de una orden de comparendo emitida por un agente de tránsito en ejercicio de sus funciones, solicitan ser escuchados en audiencia pública, de conformidad con la normativa aplicable.
- Expedición de licencias de conducción: gestionar la expedición de licencias de conducción a las personas que cumplen los requisitos establecidos para su obtención. Actualmente, este servicio se encuentra suspendido.
- Expedición de licencias de tránsito: gestionar los trámites relacionados con la legalización ante las autoridades de tránsito y transporte de la situación del propietario, tenedor o poseedor del automotor.
- Otros trámites: atender los requerimientos y trámites relacionados con el parque automotor matriculado en el departamento, tales como traspasos, duplicados de licencias, cancelación de matrículas, entre otros.

En el contexto de la seguridad de la información, el diagnóstico realizado evidenció que la Oficina de Tránsito cuenta con determinados mecanismos de protección asociados a servicios administrados por terceros, particularmente aquellos relacionados con los equipos proporcionados para el acceso a los servicios de la plataforma RUNT. Sin embargo, estos controles no cubren necesariamente la totalidad de los activos tecnológicos y servicios propios bajo administración de la Oficina.

Asimismo, se identificó que la Oficina no cuenta con un documento formal propio que establezca una política integral de seguridad de la información. El diagnóstico permitió identificar necesidades relacionadas con la gestión de credenciales y contraseñas, la actualización de aplicaciones y software, la gestión de copias de seguridad, el uso seguro de dispositivos móviles, la capacitación del personal y la segmentación de la red.

En relación con la infraestructura de red, se identificó que los equipos de la Oficina y los dispositivos utilizados por usuarios invitados de otras dependencias de la Gobernación comparten la misma red, sin una segmentación lógica mediante VLAN que permita establecer un aislamiento adecuado entre estos perfiles. Aunque la conectividad dispone de un firewall integrado en el router y existe redundancia mediante una conexión por antena, la ausencia

de una segmentación interna adecuada puede incrementar la superficie de exposición y facilitar la propagación de amenazas entre dispositivos conectados al mismo segmento de red.

Estas condiciones evidencian la necesidad de fortalecer los controles de seguridad de la información aplicables a los activos y servicios que se encuentran bajo la administración de la Oficina de Tránsito, mediante el diseño de políticas, procedimientos y controles orientados a reducir los riesgos identificados y mejorar la protección de la información institucional.

2.1. DESCRIPCIÓN DE LA EMPRESA A INTERVENIR

2.1.1. Misión

La Gobernación del Magdalena tiene como misión liderar la gestión pública departamental, promoviendo el Desarrollo social, económico y ambiental del Magdalena mediante la formulación y ejecución de políticas públicas eficientes, transparentes y cercanas a la ciudadanía, garantizando el uso responsable y seguro de la información institucional, y la **Oficina de Tránsito departamental del Magdalena** siendo una de su dependencia tiene como misión:

- Disminución de siniestralidad: Reducir las tasas de mortalidad y morbilidad en los corredores viales departamentales mediante pedagogía. (Gobernación del Magdalena, 2021)
- Seguridad vial: Implementar el Plan Departamental de Seguridad Vial articulado con políticas nacionales. (Gobernación del Magdalena, 2021)
- Garantía procesal: Digitalizar los comparendos y asegurar el debido proceso en audiencias públicas de tránsito. (Gobernación del Magdalena, 2021)
- Legalización de trámites: Validar, registrar y expedir licencias de tránsito de acuerdo con la normatividad vigente. (Gobernación del Magdalena, 2021)

2.1.2. Visión

La Oficina de Tránsito Departamental del Magdalena orienta su proyección institucional hacia el fortalecimiento de una movilidad segura y sostenible en el departamento, mediante acciones dirigidas a mejorar las condiciones de tránsito, promover la cultura ciudadana y fortalecer la seguridad vial.

En este marco, la Oficina contempla como principales componentes de su proyección:

- Movilidad sostenible: proyectar al departamento hacia una infraestructura de transporte segura, cómoda y accesible, bajo principios de buen gobierno. (Gobernación del Magdalena, 2021)
- Cultura ciudadana: consolidar las Brigadas de Seguridad Vial y fortalecer la participación comunitaria como mecanismos para promover la autorregulación y comportamientos seguros en las vías. (Gobernación del Magdalena, 2021)

En el desarrollo de estas funciones, la gestión de información constituye un elemento de apoyo para la prestación de los servicios y la administración de los trámites de tránsito. Por esta razón, el fortalecimiento de las prácticas de seguridad de la información en los procesos y recursos tecnológicos bajo administración de la Oficina representa un componente complementario para garantizar la adecuada protección de la información utilizada en el desarrollo de sus actividades.

2.1.3. Mapa de procesos

La Gobernación del Magdalena cuenta con un mapa de procesos institucional en el cual Tránsito y Transporte se encuentra definido como uno de sus procesos misionales. Este mapa permite establecer el contexto institucional en el que se desarrolla la gestión de la Oficina de Tránsito Departamental del Magdalena.

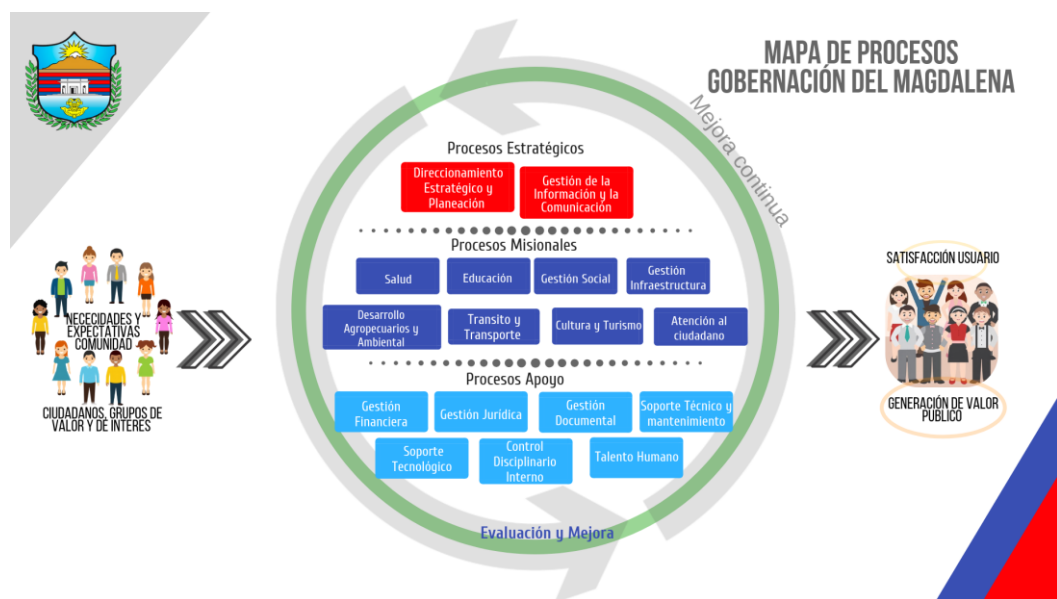


Ilustración 1: Mapas de Procesos Gobernación del Magdalena (Gobernación del Magdalena, 2021)

Sin embargo, la Oficina de Tránsito Departamental del Magdalena no cuenta con un mapa de procesos determinado que presente de manera detallada las actividades desarrolladas en la dependencia. Por esta razón, para efectos del presente proyecto de grado, se toma como referencia el mapa de procesos institucional de la Gobernación y se complementa la caracterización mediante la observación directa de las actividades desarrolladas diariamente en la Oficina.

A partir de esta observación se elaboró un diagrama del flujo de atención al usuario y gestión de los trámites, en el cual se representan las principales actividades, decisiones y recorridos que se presentan durante la atención de las solicitudes de los ciudadanos.

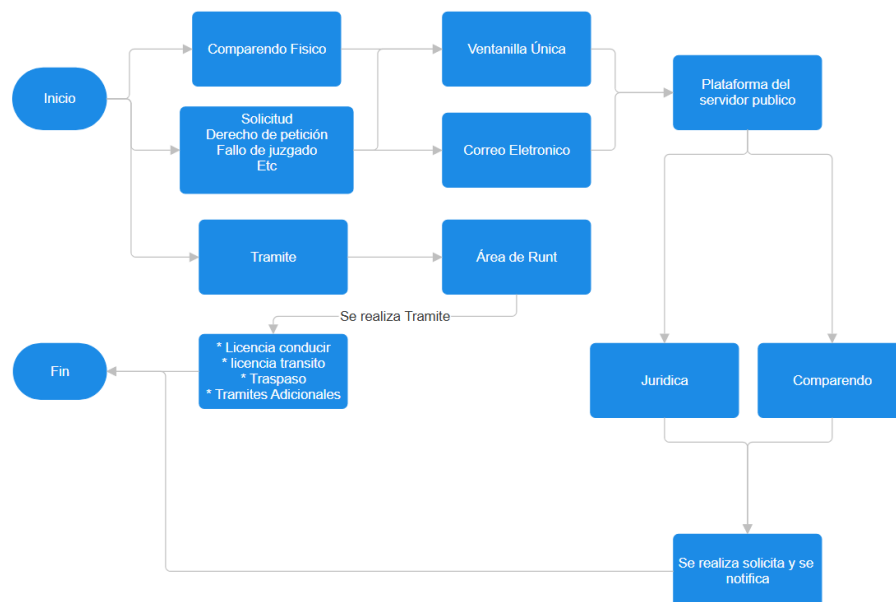


Ilustración 2 Diagrama de flujo Oficina de Tránsito Departamental del Magdalena

El flujo elaborado permite identificar las diferentes rutas que siguen las solicitudes de los usuarios, de acuerdo con el tipo de trámite o requerimiento presentado. Entre las actividades observadas se encuentran la atención de comparendos, solicitudes, trámites relacionados con licencias, traspasos, audiencias y otros servicios asociados a la gestión de tránsito.

De esta manera, el mapa institucional y el flujo elaborado permiten establecer el contexto y funcionamiento del proceso de Tránsito y Transporte, delimitando posteriormente el proceso de Gestión de Tecnologías de la Información como el ámbito específico sobre el cual se desarrolla la intervención propuesta en este proyecto.

2.1.4. Descripción del proceso a intervenir

El proceso objeto de intervención corresponde a la Gestión de Tecnologías de la Información de la Oficina de Tránsito Departamental del Magdalena, específicamente en los aspectos relacionados con la administración y protección de los recursos tecnológicos utilizados para el desarrollo de sus actividades y la prestación de los servicios asociados a los trámites de tránsito.

La Oficina cuenta con una infraestructura tecnológica compuesta principalmente por equipos de cómputo conectados mediante cableado a un switch, un punto de acceso inalámbrico (Access Point) y un router que proporciona la conectividad a Internet y dispone de funciones de firewall. Adicionalmente, cuenta con un mecanismo de redundancia de conectividad mediante una antena. La infraestructura no dispone de servidores propios para el almacenamiento de información, por lo que se utilizan servicios en la nube, como Google Drive, para la gestión y almacenamiento de información institucional.

En el desarrollo de sus actividades, los funcionarios utilizan los equipos de cómputo para acceder a aplicaciones y servicios relacionados con la gestión de los trámites de tránsito. Entre estos se encuentra un aplicativo web implementado mediante contratación externa, en el cual los usuarios gestionan los trámites que les son asignados. Este mecanismo establece restricciones de acceso a cada funcionario.

Asimismo, el personal utiliza dispositivos móviles que se conectan a la red interna y permiten el acceso a aplicaciones web institucionales y el intercambio de información relacionada con las actividades de la Oficina. En algunos casos, se utilizan aplicaciones de mensajería para compartir información asociada a la gestión de los trámites y solicitudes de los usuarios, lo que constituye un aspecto relevante para la gestión de la seguridad de la información.

La conectividad de la Oficina se encuentra integrada a la infraestructura de red utilizada por otras dependencias de la Gobernación. Actualmente, los equipos internos de la Oficina y los dispositivos utilizados por usuarios invitados de otras dependencias comparten la misma red, sin una segmentación lógica mediante VLAN que permita establecer un aislamiento diferenciado entre estos perfiles.

En cuanto a los servicios administrados por terceros, la Oficina utiliza equipos proporcionados por el Consorcio RUNT para acceder a los servicios de la plataforma RUNT. Estos equipos

cuentan con mecanismos de seguridad establecidos dentro del entorno administrado por dicho proveedor. Por tanto, el proceso presenta una diferencia entre los controles de seguridad asociados a servicios administrados por terceros y aquellos aplicables a los recursos tecnológicos y prácticas que se encuentran bajo la administración directa de la Oficina.

El diagnóstico del proceso se orienta, por tanto, a determinar las brechas existentes en la gestión de la seguridad de la información de los recursos propios de la Oficina, considerando aspectos como la gestión de credenciales y contraseñas, actualización de aplicaciones y software, segmentación de la red, uso seguro de dispositivos móviles, gestión de copias de seguridad y capacitación del personal. Los resultados de este diagnóstico servirán como base para el diseño de las medidas y políticas de seguridad propuestas en el proyecto.

2.1.5. Descripción del problema que presenta el proceso

El problema es una brecha en la gestión de la seguridad de la información de los recursos tecnológicos que se encuentran bajo la administración de la Oficina de Tránsito Departamental del Magdalena. Si bien existen mecanismos de seguridad implementados por terceros para servicios específicos, como los equipos suministrados para el acceso a la plataforma RUNT, estos controles están asociados a dichos servicios y no abarcan de manera integral los recursos tecnológicos, procesos y prácticas que son responsabilidad propia de la Oficina.

El diagnóstico realizado permitió identificar la ausencia de lineamientos formales para la gestión de credenciales y contraseñas, actualización de aplicaciones y software, copias de seguridad, uso seguro de dispositivos móviles y capacitación del personal en seguridad de la información. Asimismo, se evidenció que los equipos de la Oficina comparten la misma red con dispositivos utilizados por usuarios invitados de otras dependencias, debido a que actualmente no existe una segmentación lógica mediante VLAN que permita separar estos usuarios y establecer controles de comunicación entre los segmentos.

Estas condiciones incrementan la exposición de los recursos tecnológicos y de la información institucional frente a riesgos como accesos no autorizados, propagación de amenazas dentro de la red, pérdida de información y divulgación inadecuada de información institucional.

Además, la ausencia de lineamientos y controles formalmente definidos dificulta que la Oficina cuente con criterios establecidos para gestionar estos riesgos de manera preventiva.

Por lo anterior, el proyecto se orienta a diagnosticar las brechas de seguridad existentes y diseñar propuestas de medidas de seguridad de la información para los recursos tecnológicos bajo administración de la Oficina. Las propuestas estarán orientadas a fortalecer los controles internos, reducir la exposición de los recursos tecnológicos y establecer lineamientos acordes con los riesgos identificados, sin contemplar la implementación o puesta en operación de las medidas diseñadas.

3. ESTABLECIMIENTO DE PLANES DE ACCIÓN PARA LA SOLUCIÓN DEL PROBLEMA

En esta sección, se establecen objetivos claros y específicos que busca que el plan de acción diseñado para atender el problema de seguridad de la información identificado en la Oficina de Tránsito Departamental del Magdalena, procurando que estos se encuentren directamente alineados con el problema de identificado y con la solución de la propuesta.

Posteriormente, se hace presentación de una descripción detallada para la solución planteada, explicando de la forma que se debe abordar la causa raíz del problema y contribuir al mejoramiento del desempeño del proceso afectado.

A continuación, se desarrolla una secuencia de actividades para la implementación de la solución, organizadas de manera cronológica y coherente. Para cada actividad se especifican los recursos humanos, materiales tecnológicos y financieros requeridos para garantizar una ejecución efectiva y eficiente del plan. Asimismo, cada actividad deberá contar con criterios de medición que permitan verificar su cumplimiento y su contribución al logro de los objetivos establecidos.

Finalmente, el plan deberá orientarse hacia un proceso de mejora continua y sostenible, de manera que las acciones implementadas respondan a las necesidades de la organización y contribuyan al fortalecimiento permanente de la seguridad de la información.

3.1. ESTABLECIMIENTO DE OBJETIVOS

Plan de acción orientado al logro de 3 objetivos

1. Diseñar una propuesta de política de seguridad de la información para la Oficina de Tránsito Departamental del Magdalena, que incluya lineamientos para la gestión de credenciales y contraseñas, actualización de software y aplicaciones, copias de seguridad y uso seguro de dispositivos móviles, con el propósito de establecer criterios de protección aplicables a los recursos tecnológicos de uso interno de la Oficina.
2. Diseñar una propuesta de segmentación lógica de la red interna para la Oficina de Tránsito Departamental del Magdalena mediante VLAN, separando los equipos propios de la dependencia de los dispositivos utilizados por usuarios invitados de otras dependencias de la Gobernación, con el propósito de reducir la superficie de exposición y limitar la propagación de posibles incidentes de seguridad.
3. Diseñar un programa de capacitación y concientización en seguridad de la información dirigido al personal de la Oficina de Tránsito Departamental del Magdalena, que incluya buenas prácticas de seguridad, identificación de phishing, manejo seguro de dispositivos móviles y uso adecuado de aplicaciones de mensajería empleadas en la gestión de trámites, con el propósito de fortalecer el factor humano que es un componente crucial en la protección de los activos de información.

3.2. DESCRIPCIÓN DE LA SOLUCIÓN

La solución propuesta contempla tres componentes complementarios. En primer lugar el diseño de una **política de seguridad de la información** aplicable a los recursos propios de la Oficina de Tránsito Departamental del Magdalena, que contemple requisitos mínimos de contraseñas (longitud, complejidad, vigencia y bloqueo por intentos fallidos), lineamientos para la actualización periódica de aplicaciones, un esquema de copias de seguridad periódicas de la información almacenada en la nube, reglas de uso seguro para los dispositivos móviles y manejo de aplicaciones de mensajería utilizadas para la gestión de solicitudes.

En segundo lugar, se planteara un diseño de una propuesta de **segmentación lógica de la red interna** mediante VLAN, de forma que los equipos de cómputo propios de la dependencia queden aislados de los dispositivos de usuarios invitados de otras dependencias de la Gobernación que actualmente comparten la misma red, estableciendo reglas de acceso que limiten la comunicación entre segmentos sin afectar la conectividad requerida hacia los servicios administrados por terceros (como los equipos del Consorcio RUNT), la viabilidad técnica de la segmentación deberá considerar las capacidades del router y del switch actualmente disponibles.

En tercer lugar, se plantea el **diseño un programa de capacitación y concientización** dirigido a los funcionarios de la Oficina de Tránsito Departamental del Magdalena, orientado a fortalecer el factor humano frente a los riesgos identificados: manejo de contraseñas, identificación de intentos de phishing, uso adecuado de dispositivos móviles y aplicaciones de mensajería, y reporte oportuno de incidentes de seguridad.

En conjunto, estos tres componentes buscan atender las principales brechas identificadas durante el diagnóstico, fortaleciendo los controles y lineamientos de seguridad de los recursos tecnológicos bajo administración de la Oficina. La propuesta comprende el diseño de las políticas, procedimientos, arquitectura de segmentación y programa de capacitación.

3.3. SECUENCIA DE ACTIVIDADES PARA EJECUCIÓN DE LA SOLUCIÓN

1. Revisión de los resultados del diagnóstico y levantamiento de requerimientos y elaboración del borrador de la política de seguridad de la información (contraseñas, actualización de software, copias de seguridad y uso de dispositivos móviles) para la Oficina de Tránsito Departamental del Magdalena.
2. Elaboración de la propuesta de política de seguridad de la información, incluyendo lineamientos para la gestión de contraseñas, actualización de software y aplicaciones, copias de seguridad y uso seguro de dispositivos móviles.
3. Diseño de la propuesta de segmentación lógica de la red mediante VLAN, definiendo los segmentos requeridos, las reglas de comunicación y los mecanismos de control entre los equipos propios de la Oficina y los dispositivos de usuarios invitados. La propuesta tendrá en cuenta la infraestructura de red actualmente disponible.

4. Diseño de la propuesta de procedimiento para copias de seguridad, estableciendo criterios de periodicidad, alcance, almacenamiento, protección, recuperación y verificación de los respaldos, de acuerdo con las necesidades y características de la información gestionada por la Oficina.
5. Diseño del programa de capacitación y concientización en seguridad de la información, incluyendo contenidos relacionados con gestión de contraseñas, phishing, manejo de información, dispositivos móviles, aplicaciones de mensajería y reporte de incidentes.
6. Integración y presentación del plan de acción, consolidando las políticas, procedimientos, propuesta de segmentación y programa de capacitación, junto con los criterios de medición y recomendaciones para una eventual implementación futura.

3.4. DESCRIPCIÓN DE RECURSOS NECESARIOS PARA LA EJECUCIÓN DE LA SOLUCIÓN

Para el desarrollo de la propuesta para la Oficina de Tránsito Departamental del Magdalena se requiere disponer de recursos humanos, tecnológicos y financieros que permitan llevar a cabo las actividades de levantamiento de información, análisis de las condiciones actuales, diseño de las soluciones y elaboración de la documentación. Estos recursos estarán orientados a garantizar que las propuestas relacionadas con la política de seguridad de la información, la segmentación lógica de la red y el programa de capacitación sean diseñadas de acuerdo con las necesidades y características de la Oficina.

Es importante aclarar que el presente proyecto se limita al diseño de una solución de seguridad de la información, por lo cual no contempla la adquisición, configuración ni implementación de los controles tecnológicos propuestos. En consecuencia, los recursos descritos corresponden principalmente a aquellos necesarios para desarrollar el diagnóstico, elaborar los diseños, documentar las propuestas y validar su con las condiciones actuales de la Oficina de Transito Departamental del Magdalena.

- **Recursos humanos:**
 - **Responsable del proyecto:** encargado de coordinar las actividades de levantamiento de información, análisis de las condiciones actuales, identificación de brechas y elaboración de las propuestas de seguridad.

- **Personal con conocimientos en seguridad de la información:** brindará apoyo en el análisis de los riesgos, definición de controles y elaboración de las políticas y procedimientos relacionados con la seguridad de la información.
 - **Personal técnico de TI:** proporcionará información sobre la infraestructura tecnológica y de red existente, incluyendo las características del router, switch, access point y equipos de cómputo, como insumo para el diseño de la propuesta de segmentación mediante VLAN.
 - **Personal de la Oficina de Tránsito Departamental del Magdalena:** suministrará información sobre los procesos, actividades diarias, manejo de la información, utilización de los recursos tecnológicos y prácticas actuales relacionadas con contraseñas, actualización de software, copias de seguridad, dispositivos móviles y manejo de información institucional.
- **Recursos tecnológicos**
 - **Equipos de cómputo:** utilizados para el análisis de la información, elaboración de documentos, diseño de políticas y procedimientos.
 - **Router existente:** se analizarán las características y capacidades técnicas como insumo para elaborar la propuesta de segmentación lógica de la red mediante VLAN. No se contempla su configuración dentro del proyecto.
 - **Switch existente:** se realizará una revisión de sus características y capacidades para determinar su consideración dentro del diseño de la propuesta de segmentación de red. No se contempla su configuración dentro del proyecto.
 - **Access point existente:** será considerado dentro del análisis de la infraestructura actual de conectividad para determinar su relación con la propuesta de segmentación lógica.
 - **Información de la infraestructura de red:** comprende la información disponible sobre los equipos, conectividad y distribución actual de la red, necesaria para representar las condiciones existentes y elaborar el diseño propuesto.
 - **Herramientas de documentación:** serán utilizadas para elaborar las políticas, procedimientos, matrices, informes y demás documentos que conforman la solución propuesta.

- **Herramientas de diagramación:** permitirán representar gráficamente la infraestructura actual y la propuesta de segmentación lógica mediante VLAN.
- **Material de capacitación:** comprende presentaciones, guías, documentos y material de apoyo que serán utilizados para estructurar el programa de capacitación y concientización dirigido al personal.
- Recursos financieros
 - **Recursos para desplazamientos:** en caso de ser necesarios, permitirán realizar visitas a la Oficina para actividades de levantamiento y validación de información.
 - **Recursos para material de capacitación:** destinados a la elaboración o reproducción de material informativo y educativo relacionado con las buenas prácticas de seguridad de la información.
 - **Recursos para herramientas de software:** en caso de requerirse herramientas con licencia para la elaboración de diagramas, documentación o material de capacitación.
 - **Costos de implementación futura:** no hacen parte de la ejecución del presente proyecto. Sin embargo, de manera referencial, podrán identificarse posibles costos asociados a una futura implementación, tales como actualización o adquisición de equipos de red, herramientas de seguridad, soluciones de respaldo y actividades de capacitación especializada.

4. DEFINICIÓN DEL ALCANCE DE LA SOLUCIÓN, PARTES INTERESADAS, CRONOGRAMA Y PRESUPUESTOS.

En esta sección se define el alcance de la solución propuesta para el fortalecimiento de la seguridad de la información en la Oficina de Tránsito Departamental del Magdalena, se identifican las partes autorizadas y la responsabilidad de cada actividad, y se presentan el cronograma y el presupuesto de ejecución del proyecto, iniciando definiendo el alcance de la solución propuesta, especificando los límites, objetivos específicos y resultados esperados de la intervención. A continuación, identifique las partes interesadas clave y a los responsables de cada actividad dentro del plan de acción, asegurando que los roles y las responsabilidades estén claramente asignados para una ejecución coordinada. Elabore un cronograma detallado que muestre la secuencia temporal de cada actividad, indicando fechas de inicio y fin, así como

los hitos clave que permitirán evaluar el progreso de la implementación. Finalmente, desarrolle un presupuesto que desglose los recursos financieros necesarios para cada fase del proyecto, justificando cada costo de manera que se optimice el uso de los recursos y se garantice la viabilidad de la solución. Asegúrese de que esta planificación detallada promueva una implementación eficiente y permita una evaluación continua del avance y los resultados alcanzados.

4.1. ALCANCE FINAL DE LA SOLUCIÓN

En esta sección se define el alcance de la solución propuesta para el fortalecimiento de la seguridad de la información en la Oficina de Tránsito Departamental del Magdalena, se identifican las partes interesadas y los responsables de cada actividad contemplada en el plan de acción, y se presenta el cronograma y presupuesto asociados al desarrollo del proyecto.

Inicialmente, se establece el alcance de la solución, delimitando por los objetivos, las actividades y los resultados esperados. también se identifican las partes interesadas que intervienen en el desarrollo de las diferentes actividades y se asignan las responsabilidades correspondientes, con el fin de que se realice una ejecución organizada y coordinada del proyecto.

También, se presenta el cronograma que establece una serie de actividades, distribuidas durante el periodo de ejecución del proyecto, junto con los principales hitos para realizar el seguimiento de su desarrollo o avance, finalmente se presenta el presupuesto de los recursos necesarios para llevar a cabo el desarrollo de las actividades de levantamiento de información, análisis, diseño y documentación de la solución propuesta.

Es importante aclarar que el presente proyecto solo se limitara al diseño de la solución y no contempla su implementación, por lo que las actividades, recursos y presupuesto definidos a continuación en este capítulo corresponden al desarrollo de la propuesta. Las acciones relacionadas con la posible implementación a futuro de las medidas diseñadas podrán ser consideradas posteriormente por la Oficina de Tránsito Departamental del Magdalena y las dependencias responsables de su ejecución.

4.2. IDENTIFICACIÓN DE RESPONSABLES DE LAS ACTIVIDADES PARA EJECUCIÓN

- **Jefe de la Oficina de Tránsito Departamental del Magdalena:** estará a cargo de la revisión y la validación de las propuestas diseñadas, especialmente de la política de seguridad de la información, y podrá determinar su pertinencia para las necesidades de la Oficina.
- **Encargado de TI o responsable de seguridad de la información:** Facilitará el levantamiento de información ya que suministrará información técnica relacionada con los recursos tecnológicos, infraestructura de red y prácticas actuales de seguridad, y participará en la revisión técnica de las propuestas elaboradas.
- **Personal de la Oficina de Tránsito Departamental del Magdalena:** Servirán como fuente primaria de información sobre los procesos, las prácticas y uso de los recursos tecnológicos, la información que suministren permitirá el diseño de las políticas, procedimientos y programa de capacitación.
- **Equipo de estudiantes (autores del proyecto):** Responsables de realizar el levantamiento de la información, el análisis de las condiciones actuales de la Oficina de Tránsito Departamental del Magdalena, el diseño de las políticas y procedimientos, elaboración de la propuesta de segmentación lógica mediante VLAN, el diseño del programa de capacitación y elaboración de los documentos y entregables establecidos en el cronograma.

4.3. CRONOGRAMA DE EJECUCIÓN

El cronograma de desarrollo del proyecto se establece para desarrollarse en un periodo de cinco meses, durante los cuales se desarrollarán de manera progresiva las actividades necesarias para el diseño de la solución de seguridad de la información propuesta para la Oficina de Tránsito Departamental del Magdalena.

Entre las actividades se encuentran:

- El levantamiento de requerimientos y elaboración de la propuesta de política de seguridad de la información, su posterior revisión y validación.
- El diseño técnico de la propuesta de segmentación lógica de la red mediante VLAN.
- El diseño del esquema de copias de seguridad.
- Estructuración del programa y el material de capacitación y concientización.

Finalmente, se contempla la consolidación y socialización de la propuesta de seguridad como la actividad final del proyecto. Es importante señalar que las actividades programadas corresponden al diagnóstico, diseño, documentación y validación de las propuestas, por lo que no se contemplan en ninguna medida la implementación técnica de los controles ni la puesta en operación de las medidas de seguridad diseñadas.

La distribución de estas actividades se presenta o detallan en la Tabla 1.

Tabla 1. Cronograma de actividades.

Actividad	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9
1.Levantamiento de requerimientos y elaboración del borrador de la política de seguridad	x	x							
2.Revisión y validación de la propuesta de política de seguridad.		x							
3.Diseño técnico de la propuesta de segmentación de red (VLAN y reglas de acceso).		x	x						
4.Diseño del esquema de copias de seguridad.			x						
5.Diseño del programa y material de capacitación			x	x					
6.Validación del programa de capacitación y material educativo				x					
7.Consolidación y socialización de la propuesta de					x				

seguridad de la información.									
------------------------------	--	--	--	--	--	--	--	--	--

4.4. PRESUPUESTO

El presupuesto que se estima para el desarrollo del presente proyecto contempla los recursos necesarios para realizar las actividades de levantamiento de información, análisis, diseño, documentación y validación de la solución de seguridad de la información propuesta para la Oficina de Tránsito Departamental del Magdalena. según se detalla en la Tabla 2.

Ya que el alcance del proyecto se limita solamente al diseño de la solución y no contempla en ninguna medida su implementación, no se incluirán dentro del presupuesto los costos asociados a la adquisición de equipos de red, la configuración de VLAN, actualización o reemplazo de la infraestructura tecnológica, la adquisición de soluciones de seguridad, contratación de servicios para la implementación de copias de seguridad, el licenciamiento de plataformas adicionales ni la ejecución de jornadas de capacitación al personal. Estos elementos podrán ser considerados por la entidad en una posible fase futura de implementación.

Para la definición de los costos de cada actividad se calcularán, haciendo uso de la formula:

Costo de la actividad = número de personas x horas estimadas x tarifa por hora.

Para la elaboración del presupuesto, se establece una tarifa de referencia de \$ 50.000 pesos m/cte. por hora de trabajo, utilizada como base para estimar el valor del recurso humano requerido para el desarrollo de las actividades.

Tabla 2. Presupuesto.

Rubro	Valor
Levantamiento de información, análisis y diseño de la política de seguridad y propuesta de segmentación de red. (40 horas por integrante; 2 integrantes = 80 horas-persona)	\$4.000.000 pesos m/cte.

Diseño y material del programa de capacitación y concientización. (12 horas por integrante; 2 integrantes = 24 horas-persona)	\$1.200.000 pesos m/cte.
Diseño del procedimiento de copias de seguridad. (5 horas por integrante; 2 integrantes = 10 horas-persona)	\$500.000 pesos m/cte.
Documentación, diagramación y consolidación de la propuesta. (3 horas por integrante; 2 integrantes = 6 horas-persona)	\$300.000 pesos m/cte.
Desplazamientos para levantamiento y validación de información	\$500.000 pesos m/cte.
Imprevistos (10 %)	\$650.000 pesos m/cte.
Total	\$7.150.000 pesos m/cte.

5. REFERENCIAS BIBLIOGRÁFICAS

- Fortinet, Inc. (s.f.). *Segmentación de red*. Recuperado el 10 de agosto de 2026, de <https://www.fortinet.com/lat/resources/cyberglossary/network-segmentation>
- Gobernacion del Magdalena. (2021). *Gobernacion del Magdalena*. Recuperado el 4 de agosto de 2026, de Mapa de Procesos: <https://www.gobernaciondelmagdalena.gov.co/transparencia-resolucion-1519-de-2020/transparencia-informacion-de-la-entidad/mapa-de-procesos/>
- Gobernación del Magdalena. (2021). *Oficina de Tránsito y Transporte*. Obtenido de Oficina de Tránsito y Transporte: <https://www.gobernaciondelmagdalena.gov.co/oficina-de-transito-y-transporte/>
- Ministerio de tecnologías de la información y las comunicaciones (TIC). (21 de abril de 2025). Lineamientos de Roles y Responsabilidades. (V 5.0). Dirección de Gobierno Digital. Recuperado el 21 de agosto de 2026, de https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-401771_recurso_1.pdf
- Organización Internacional de Normalización (ISO). (Octubre de 2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements - ISO/IEC 27001. Recuperado el 13 de agosto de 2026
- Scarfone, K., & Hoffman, P. (septiembre de 2009). Guidelines on Firewalls and Firewall Policy. ((NIST Special Publication 800-41 Rev. 1)). (N. I. (NIST), Ed.) Obtenido de <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf>